AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

1-10. (Cancelled).

11. (New) A method of controlling a network entity of a mobile communication network and a mobile station, wherein said network entity and said mobile station are adapted to conduct a plurality of predetermined message exchange procedures in the course of which predetermined messages are exchanged between said network entity and said mobile station depending on the given procedure, where said predetermined messages may be encrypted, an encrypted message being any message of which at least a part is encrypted, and where said network entity and said mobile station are adapted to conduct one or more encryption key generation procedures during which the network entity and the mobile station generate and store respective corresponding encryption keys in order to be able to encrypt and decrypt exchanged messages, said method comprises the steps of:

if said network entity receives a message from said mobile station, determining whether said received message is encrypted;

if the received message is encrypted, determining whether a correct encryption key for decrypting said message is available to said network entity and, if no correct key is available, sending a predetermined triggering message to said mobile station; and

upon receiving said predetermined triggering message, said mobile station interrupting the procedure in the course of which it sent the encrypted message for which the network entity did not have a correct key, and initiating an encryption key generation procedure.

12. (New) The method according to claim 11, wherein said messages are arranged such that they have a first part and a second part, said first part being an

unencrypted part that is not allowed to be encrypted, and said second part being encryptable.

13. (New) The method according to claim 12, wherein said messages are arranged such that said first part contains an encryption indication of whether said second part is encrypted or not, and said determining of whether the second part of said received message is encrypted or not is achieved by analysing said encryption indication.

14. (New) The method according to claim 12, wherein said messages are arranged such that said first part contains a message type identifier identifying the type of the message, and after having received a message from said mobile station, said network entity identifies the message type of said received message from the message type identifier and determines whether said identified message type belongs to a predetermined category, and sends said predetermined triggering message to said mobile station only if the message type of said received message falls into said predetermined category.

15. (New) The method according to claim 11, wherein said one or more encryption key generation procedures comprise obtaining an encryption base value commonly available to said network entity and said mobile station at the time of conducting said encryption key generation procedure, and generating corresponding encryption keys in said network entity and said mobile station on the basis of said encryption base value.

16. (New) The method according to claim 15, wherein said encryption base value is a regularly changed value that is broadcast by said network to listening mobile stations.

17. (New) The method according to claim 11, wherein said encryption key generation procedure is conducted as a part of a registration procedure of said mobile station with said network entity.

18. (New) A mobile station adapted to operate with a mobile communication network, said mobile station comprising:

an encryption key generator) for generating a encryption key;

an encryption key memory for storing a generated encryption key;

a message encryptor/decryptor for encrypting messages sent to said mobile communication network and decrypting messages received from said mobile communication network using a stored encryption key, an encrypted message being any message of which at least a part is encrypted; and,

a controller for controlling the operation of said mobile station, said controller being adapted to perform one or more predetermined message exchange procedures with said mobile communication network in the course of which said mobile station sends predetermined types of messages to said mobile communication network and waits for predetermined corresponding types of messages from said mobile communication network, said controller furthermore being arranged to identify the receipt of a predetermined triggering message from said mobile communication network during the course of an ongoing message exchange procedure, and in response to said predetermined triggering message interrupting the ongoing message exchange procedure and initiating an encryption key generation procedure.

19. (New) The mobile station according to claim 18, wherein said controller is arranged to conduct said encryption key generation procedure as a part of a registration procedure of said mobile station with said mobile communication network.

20. (New) A network apparatus of a mobile communication network arranged to communicate with a mobile station, said network apparatus comprising:

an encryption key generator for generating a encryption key;

an encryption key memory for storing a generated encryption key;

a message encryptor/decryptor for encrypting messages sent to said mobile station and decrypting messages received from said mobile station using a stored encryption key, an encrypted message being any message of which at least a part is encrypted; and,

a controller for controlling the communication between said network entity and said mobile station, said controller being arranged to determine whether messages received from said mobile station are encrypted or not, and if a received message is encrypted, determining whether a correct key for decrypting said message is available to said network entity, and if no correct key is available, sending a predetermined triggering message to said mobile station for triggering an immediate encryption key generation procedure in said mobile station.

* * *